Malware analysis with multiple features

Abstract:

Malware analysis process is being categorized into static analysis and dynamic analysis. Both static and dynamic analysis have their own strengths and weaknesses. In this paper, we present a tool written in Python programming language called as pingaji, which could assist the work of malware analyst to get the static features of malware. pingaji contains several modules - Application Programming Interface (API) calls extractor, binary entropy information, anti virtual machine and anti debugger detector and XOR encrypted strings decrypt or. pingaji was developed in order to assist our work in getting malware features. pingaji is focusing on ripping Microsoft Windows executable binaries' malicious features.